November 18, 1997

TO: Dwight Dively, Director, Executive Service Department
Mike Herrin, Project Director, SFMS Redevelopment Project

FROM: Nora Masters, City Auditor

SUBJECT: Issues of Interest to the Office of City Auditor Regarding the Development of Large Computer Applications

The SFMS redevelopment project (Summit) is vital to both the City's accounting operations and to the State Auditor's and our reliance upon the City's accounting information for our audits. As you know from our discussions and our role as an *ex officio* member of the Summit Steering Committee, my office is committed to helping the City ensure that decisions regarding the redevelopment of SFMS are made using the best data available, and that all applicable City policies and good public administration practices are followed. I have prepared the attached "Issues of Interest," drafts of which you reviewed in January and May 1997, to highlight areas of particular concern to the Office of City Auditor, and the types of information my office may want to review before I approve the acceptance of any new or redeveloped financial system.

Steps 1 through 5 of the "Issues of Interest" paper focus on the selection process. Since we attended many of the Steering Committee meetings and vendor presentations, and reviewed many of the documents prepared to reach the procurement decisions, we do not anticipate a need to revisit or audit the selection process at this time. Please call me at 233-0088 or Susan Cohen at 233-1093 if you have any questions or comments about the attached documents or the role we wish to play in the SFMS redevelopment project.

cc: Mayor Norm Rice
Councilmembers

Attachments: Issues of Interest
Auditor's Role in Computer System Applications

Office of City Auditor's
Involvement in the Acquisition of New Computer Systems

The Office of City Auditor's basic mission is to provide independent and objective analysis of City programs and functions. There are certain roles the Office of City Auditor staff can play in the acquisition of new computer systems which are compatible with the Office's basic mission and other roles which are incompatible. The following describes these roles.

Roles the Office of City Auditor Staff Can Play

- Attend appropriate meetings of the project team.
- Review all available documentation pertaining to controls.
- Evaluate reporting, input, and processing features to ensure adequacy of controls.
- Monitor compliance with organization standards.
- Provide advice, as necessary, on issues of controls, standards, documentation, etc.
- Determine if the vendor search and analysis processes are performed adequately.
- Review the test plan and implementation plan for adequacy.
- Participate in the acceptance tests and final approval process.
- Perform a post-implementation review.
- Report to executive management and the Council on the audit issues related to the project.

Roles Audit Office Staff Should Not Play

- Establish system requirements other than audit impacting requirements.
- Develop or design system or program specifications.
- Develop the requests for proposals.
- Develop vendor-rating criteria.
- Rate the vendors.
- Design test data or develop test plans.
- Develop the implementation plans.

Issues of Interest to the Office of City Auditor Regarding the Development of Large Computer Applications

INTRODUCTION

This paper and its companion Audit program was developed to guide the Office of City Auditor in its auditing of the City's acquisition of large computer systems and to communicate to Departments the issues of importance to the Office. This paper provides a generic discussion of the documentation and controls the Office of City Auditor may want to review in evaluating (1) the acquisition and (2) the day-to-day operations of the computerized financial system of the new Seattle Financial Management System or other major computer systems. Our concern is to ensure that -- prior to acceptance and approval -- the acquisition and operations of the system receive appropriate management and documentation and that the system builds in appropriate internal controls and adequate "auditibility." We expect that the project team and department management will develop the documentation and build in the controls we are looking for as a normal part of their work and will not see them as some "add-on" requiring additional effort. The information in this document is based on standard, generally accepted audit practices for computer acquisition. The main audit objectives include ensuring fair and thorough competition for selecting vendors, the development of proper specifications for the system, and the appropriate safeguards to ensure that the accepted system meets the City's needs.

I. SYSTEM ACQUISITION MANAGEMENT

To enable our office to determine the effectiveness of management controls for the acquisition of new application systems, the conversion of information from old systems to the new system, and to conclude that the new system will satisfy user and auditor needs prior to acceptance and approval, the Office of City Auditor may want to review the following.

A. Procurement Process

The auditor's review of the procurement process may include reviewing the request for services, the systems requirements definition, the feasibility report, the request for proposals, and the documentation of the

1. Request for Services

The first step in any acquisition or development project should be the development of a request for services. Generally. the request comes from the user department and is prompted by some weakness in the current system or procedures (e.g., the system cannot handle new regulatory requirements, does not provide adequate and timely customer services, does not provide required information, etc.). However, the request

may also be initiated by data processing or other personnel in response to operational weaknesses or problems.

2. Systems Requirements Definition

Generally developed once management has given the initial approval for the project's initiation phase,[1] this document should contain:

- a description of the current system, along with an analysis of whether or not the present system is adequate to serve as a basis for studying the needs of the proposed system;
- a general analysis of the requirements of the new system, including business needs, data requirements, regulatory requirements and security needs;
- an analysis of how each system requirement will affect and interface with other systems in the organization; and
- a general discussion of system design, including the technology to be utilized and conversion migration issues.

3. Feasibility Report

The feasibility report should include the team's recommendation relative to alternative approaches, vendors, and software packages and provide the following information:

- background related to the project proposal (for example, changes in organizational environment, needs, opportunities, goals, statutory requirements);
- the primary objectives of the project (for example, problem solutions, service enhancements, response to statutory requirements);
- the alternatives evaluated;
- the recommended solution and the reasons for the team's recommendation, including a discussion of the benefits of the new system over the old system, new system costs versus present system costs, and the approximate implementation cost.
- entities affected by the proposed project, including programs and subprograms, organizational units, outside agencies, and customers (for example, constituencies, taxpayers);
- organizational impact of the project -- how the project may affect such aspects of the organization as work processes, training needs, job content, and organizational structure;
- conformity of the project with the agency's information technology goals, particularly its focus and its vision of technology infrastructure;

[1] Formal approval of the project as a whole should await completion of the feasibility study.

- project management, including roles and responsibilities, the decision-making process, management qualifications, project team organization, and quality assurance strategies;
- estimated time frame and work plan, overall and by project phase, through implementation, identifying major tasks, staff resources required, and key decision points; and
- the principal risks this project faces and how the organization will manage these risks;

4. Request for Proposal

The Request for Proposal helps document how well the organization managed the procurement process. It generally includes the following:

- User requirements (for example, specific accounting/business practices, on-line access and inquiry, specific calculation methods, content and timing of reports);
- Technical requirements (for example, program languages, data access approach, operating system compatibility, hardware compatibility, server and workstation requirements, network requirements);
- Processing/performance requirements (for example, response time, batch processing windows, current and future volume capabilities;
- Security requirements (for example, accuracy, privacy, and access controls for data files, programs, workstations; micro-to-mini or micro-to-mainframe computer links, network access controls and backup, recovery procedures and alternatives, and encryption);
- Audit requirements (for example, audit modules, user exits at critical processing points to allow insertion of control routines, paper and/or electronic management trails); and
- Documentation requirements (for example, for user procedures, programs, operations).

5. Documentation Of The Vendor Evaluation Process

Documentation of the vendor evaluation process, like the Request for Proposals, provides evidence of how well the agency managed the procurement process. While the Project Management Team will specify its own evaluation criteria, vendor evaluations generally consider the following:

- Vendor's ability to meet the defined system requirements (see Systems Requirements Definition above);
- Vendor's financial stability, experience, and number of existing users;
- Vendor's responsiveness to user problems (based upon information from existing users);

- Amount of training and conversion support provided by the vendor;
- Quality of vendor's documentation;
- Vendor's response to items in the Request for Proposal (above);
- Analysis of all associated costs (including hardware upgrades required to accommodate the software); and
- Reference checks.

B. Managing Implementation

The auditor's review of the implementation process may include project management, installation of acquired software, the interface programs need to facilitate information transfer between the old system and the new system as well as other systems, and the test plan.

1. Documentation of Project Management

A project chart or schedule that identifies:

- all of the major tasks that need to be performed;
- major milestones or checkpoints;
- budget to actual expenditures;
- expected completion date;
- assigned responsibilities by individual or group;

2. Installation Procedures For Acquired Software

A document describing how acquired software was installed, including such information as:

- whether the vendor provided both source and executable code;
- whether the source code for *each* program was recompiled to produce new object code and the object code then linked (so as to avoid future problems in compiling production programs);
- whether only those programs and modules in the new system that will be utilized were installed (to save disk space, increase efficiency and avoid confusion); and
- whether initialization parameters or operating system parameters were changed during installation.

3. Documentation Of Interface Programs

Documentation of any interface programs needed to facilitate information transfer between the new system and such other systems as the Human Resource Information System, Cash Receipting System, City Light's Maintenance Management and Spare Inventory Management Systems. In particular, the Office of City Auditor will be interested in:

- the process used to obtain/develop those programs; and
- whether the interface programs are separate and independent from the purchased software or the processing logic of the purchased software had to be altered to accommodate the interface programs.

4. The Test Plan

A document which provides evidence of:

- separate testing of each program before placing it into production;
- testing of all transaction codes and program logic in the entire system;
- testing of daily, weekly, monthly, quarterly, and yearly processing cycles;
- testing of all technical components in configurations representing the operating and production environments, including the environments of all customers;
- precautions taken to guarantee customer privacy if software vendor personnel will be involved in the testing and have access to "live" data;
- review and reconciliation of the output;
- acceptance testing (*Note:* An acceptance test differs from a systems test in that user personnel rather than systems personnel prepare, conduct, and review the test, commenting on system functionality, user ease and system accuracy);
- the use of independently developed test data with predefined expected outcomes (developed preferably with major users and the Office of City Auditor). Such test data will help meet the requirement of City Ordinance 116368, Seattle Municipal Code Section 20.52.060 that "The city's automated data processing and electronic data processing equipment used in processing expenditures, warrants, and other financial data shall contain controls for accurately evaluating the integrity and reliability of financial information being produced. . . . (and be) satisfactory for fiscal audit purposes." The same test data could also be used in future years when the system is audited as an existing application to ensure that inappropriate changes have not occurred in the system.

5. The Conversion Plan

The conversion plan generally includes:

- the personnel needed at conversion;
- any needs for additional data and for additional data-entry personnel;
- default values for unavailable data and the impact of these values -- particularly the affect of using a null or 0 value on trend and other management reports;
- specific tasks to be completed at conversion time (for example, picking up master files from the service bureau; running one-time conversion program; reconciling special conversion reports; converting historical data);
- assigned responsibility for conversion tasks;
- a timetable for conversion tasks;
- a plan of action if the conversion is not successful (for example, files to restore, individuals to notify); and
- how the system converts non-year-2000 date fields.

6. Documentation of Post Conversion Reconciliation

Documentary evidence that all reports and file totals were properly reconciled after conversion.

II. APPLICATION CONTROLS

This section describes the documentation of controls which the Office of City Auditor will expect to find in the new system, indicating both the areas in which system controls should be present and the specific controls needed.

1. Identification of Input Classifications and Data Elements

This documentation identifies all input classifications, including their nature and impact (for example, monetary vs. non-monetary transactions, customer information vs. statistical data, temporary vs. permanent). Also a data model which defines the source and use for each and all data elements

2. Batch Input Controls

This documentation summarizes the batching procedures for each input. This documentation should describe for each input batch:

- what transactions or transaction types are included;

- how the batch size and contents are determined;
- what controls ensure that batch is authorized and complete (for example, use of batch control documents, use of a record or log of the batches, use of field control totals);
- how the batch is transported to data processing and who receives it;
- how data processing personnel determine that input batches they receive are properly authorized; and
- any transmittal documents used to ensure that all input batches are properly forwarded to the reconciliation area for use during the reconciliation process.

3. On-Line Input Controls

This documentation of on-line input controls should describe the following:

- the type and number of workstations used for each input;
- procedures for entering transactions into the application (specifically, what situation causes the transaction, which personnel enter the transaction into the application, and how they enter it;
- controls that prevent unauthorized transactions from being entered into the application (including user ID and password controls);
- requirements for timely review and correction of edit errors. (Normally, on-line input routines have some built-in validity-checking capabilities that will prevent incorrect information from being entered);
- controls over data re-entered as corrections (Is this data subject to the same controls as the data in the original input?);
- retention of source documents for an adequate period of time to relate them to corresponding output records; and
- control reports, records, and procedures that ensure that all transactions submitted have been processed properly only once.

4. Output Controls

Application output varies from application to application but generally includes output reports. Additional output might include such items as accounts payable checks, invoices, and computer interface files. Appropriate documentation of output controls describes:

- the procedures data processing personnel use to determine the acceptability of output before distribution (for example, review to ensure output is complete, review of run-to-run totals, etc.)
- which user department is primarily responsible for the acceptability of an output item and for performing reconciliation of the output;
- user department procedures to verify the completeness and accuracy of output;

- records to demonstrate that appropriate personnel are regularly performing output review; output balancing and reconciliation procedures;
- records to show that all input batches/items are balanced to batch totals or other control documents to ensure (1) appropriate processing of all items or (2) proper and timely control and re-entry of rejected items; and
- a list or report for reconciliation personnel of all transactions, including interface transactions, processed by the application.

5. Controls Over Sensitive Output Items

Appropriate documentation of controls over sensitive output items will first identify which output items are sensitive (because of confidentiality or cash value). For sensitive output items, the documentation will describe:

- procedures used to control access to these items until they reach their final destination (for example, the National Automated Clearing House or another system or application);
- where unused forms and documents are physically stored and the type of physical controls appropriate (for example, blank checks should be kept in a locked cabinet or safe, and stored under dual control);
- the control records and procedures for used and blank forms (e.g., logs of pre-numbered checks, with supervisory review)
- the methods for disposing of spoiled or voided documents and of sensitive output documents or files which no longer need to be retained (see section 6 below). For example, documents may be shredded, and files erased.

If the sensitive output has a cash value or authorizes distribution of assets, appropriate documentation will describe:

- the controls over the signature plate, stamp. or other validation plate, if applicable; and
- whether these items have a maximum value limit and whether the program producing them checks each against this limit.

6. Output Retention Procedures

Appropriate documentation will:

- describe the retention policy established for various output items;
- demonstrate that the policy is in compliance with regulatory (for example, IRS) requirements.

7. Procedures for Changing Permanent Data on Live Files

Documentation should be available of all changes to permanent data on live files, both those performed outside of the normal production job stream and those performed through normal job streams.

If changes to production files are allowed outside of the normal production job stream (in emergency situations, to alleviate production problems), documentation should describe the controls that prevent the processing of unauthorized changes. The computer operations department should control all of the output and associated documentation for file changes apart from the normal job stream. Of particular importance will be the controls that ensure the creation of a record of each change showing:

- the file being changed;
- the programmer initiating the change;
- the date of the change and the reason for the change;
- the method used to make the change (for example, utility, special program);
- output from the change process (for example, parameter listings, reports);
- the supervisory review of all output;
- the authorization forms for the override of the data security software, if applicable.

When processing changes to live production files through normal job streams, user departments should document their procedures which ensure that changes have been processed as requested. This documentation should:

- identify and describe the reports of accepted changes to the files; and
- identify edit tests and error correction procedures that contribute to the accuracy of the data on the files.

8. Controls Ensuring Use of Proper Files

Documentation is needed of controls in place to ensure that proper files are used during the normal processing cycle. This documentation should describe:
what internal and external file labels are to be used:

- whether generation dating is to be used to allow the system to automatically keep track of the current version of any particular file;
- any use of run-to-run totals, which allow computer operators to check control totals before continuing with the processing; and
- user verification of totals.

9. Data Access Controls

Regardless of the procedures controlling data changes, proper control of file access is necessary to assure that those procedures are being adhered to. Documenting the controls used to restrict access to production files includes describing:

- any use of dedicated data security software (including whether it is fully implemented and whether it controls *all* production files);
- manual controls over computer tape libraries, including restrictions on access to the tape library and procedures (including the request forms and necessary authorizations) for obtaining production tapes from the library for use both in production runs and also in other than production runs;
- any standard operating system access controls for network and data access, identifying all data protected, how computer operators obtain authorization to override the password protections, and what procedures ensure all file overrides are properly authorized; and
- any application specific security

10. Application Documentation

Appropriate documentation for every computer application executed in a production mode includes:

- a system flowchart;
- a detailed program narrative for each program that explains the purpose of the program, an overview of the processing logic, and the interaction of this program with other programs in the system or with other systems;

- decision tables and flowcharts;
- detailed file formats and record layouts;
- requirements for dialog layout, describing each field's source and use;
- report layouts or samples of output reports, with descriptions of each field's source and use;
- descriptions of input and output files;
- description of on-line help functions; and
- a record of program changes, their authorizations, and effective dates.

11. Operations Documentation

Operations documentation provides computer operators with the information they require to execute current production programs (including all changes) and resolve run-time problems. It also provides necessary information relative to scheduling, output distribution, and job control language. Operations documentation should include:

- job setup and scheduling instructions;
- production job stream listing;
- operator instructions, including;
    - frequency and sequence of program execution;
    - job precedence and dependency requirements;
    - identification of input and output files;
    - estimated running times;
    - program messages and responses; and
    - restart and recovery procedures, if applicable.

12. Documentation For Audit Tests

For auditors' input/output verification tests, the input items for a selected day should be available for the auditor's inspection. If input is on-line and no original input documents are available, "capture" reports, user records, or other reports that list the input transactions should be available. If specific audit tools are available, a document should describe their purpose and capabilities and sufficient information to enable the auditor to successfully operate them.